Software Engineering Institute

An Introduction to the Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC)

Christopher Alberts
Audrey Dorofee
Robin Ruefle
Mark Zajicek

May 2014

TECHNICAL NOTE
CMU/SEI-2014-TN-005

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Homeland Security or the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0001255

Table of Contents

List of Figures

List of Tables

Acknowledgments

We would like to thank the following people for contributing to the content of this document: Jeff Carpenter, Rob Floodeen, Mike Murray, Larry Rogers, Mike Stone, and Michael Theis. We also thank the following members of the SEI technical staff for reviewing this technical note: Julia Allen, Kristi Keeler, and Ryan Meeuf. We would also like to thank Paul Ruggiero for editing this document.

Abstract

An incident management (IM) function is responsible for performing the broad range of activities associated with managing computer security events and incidents. For many years, the Software Engineering Institute's (SEI) CERT® Division has developed practices for building and sustaining IM functions in government and industry organizations worldwide. Based on their field experiences over the years, CERT researchers identified a community need for a time-efficient means of assessing an IM function. The Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC) is designed to address this need. The MRD-IMC is a risk-based approach for assessing the extent to which an IM function is in position to achieve its mission and objectives. Analysts applying the MRD-IMC evaluate a set of systemic risk factors (called drivers) to aggregate decision-making data and provide decision makers with a benchmark of an IM function's current state. The resulting gap between the current and desired states points to specific areas where additional investment is warranted. The MRD-IMC can be viewed as a first-pass screening (i.e., a "health check") or high-level diagnosis of conditions that enable and impede the successful completion of the IM function's mission and objectives. This technical note provides an overview of the MRD-IMC method.

1 Introduction

Incident management (IM) refers to all of the activities that are performed in an organization when managing computer security events and incidents [Dorofee 2008]. The term *incident management function* refers to the broad spectrum of activities associated with providing IM services. An IM function is instantiated in a set of capabilities (or practices) considered essential to protecting, detecting, and responding to incidents, as well as sustaining the IM function. These capabilities can be provided by a variety of groups, including security personnel, system and network administrators, service organizations, and computer security incident response teams (CSIRTs).

Organizational stakeholders (e.g., business-unit managers, information-technology managers, system owners, data owners, system operators, system users) have a vested interest in ensuring that systems and networks provide users with the information and services they need. Stakeholders also have a growing interest in providing information and services in a secure manner. A variety of organizational and technical assessments (e.g., audits, process assessments, risk assessments) can be used to provide insight into an organization's security posture. With respect to IM, assessments help assure stakeholders that IM services are being delivered with a high standard of quality and within acceptable levels of risk.

From our experience working with the IM community over the years, we identified a need for a time-efficient means of assessing an IM function. In 2008, we developed the Incident Management Mission Diagnostic (IMMD) [Dorofee 2008]. The IMMD was designed to provide an efficient and effective means of assessing an IM function. During the past year, we updated the IMMD and aligned it with several related assessments that have been developed by the Carnegie Mellon[®] Software Engineering Institute (SEI). That development effort produced the Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC), which is a risk-based approach for assessing an IM function.

The overarching goal of the MRD-IMC is to determine the extent to which an IM function is in position to achieve its mission and objective(s) [Alberts 2012]. To accomplish this goal, analysts applying the MRD-IMC evaluate a set of systemic risk factors (called drivers) to aggregate decision-making data and provide decision makers with a benchmark of an IM function's current state. The resulting gap between the current and desired states points to specific areas where additional investment in an IM function is warranted.

This report provides an overview of the MRD-IMC method. The overview begins with a discussion of how we view the Mission Risk Diagnostic (MRD) as a common platform for a family of assessments.

1.1 MRD Assessment Platform

Over the past several years, SEI field experience has yielded anecdotal evidence that programs and organizations throughout government and industry are unable to assess their risks effectively.

[®] Carnegie Mellon is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

For example, SEI independent assessments typically uncover significant risks that have not been brought to the attention of key decision makers within the programs and organizations that are being assessed. When decision makers are unaware of significant risks, they are unable to take action to mitigate those risks. As a result, we undertook a project to examine and improve the practice of risk assessment. When conducting this project, we leveraged the SEI's rich history in the discipline of risk management.

Since the early 1990s, the SEI has conducted research and development in the area of risk management and has applied risk management methods, tools, and techniques across the software lifecycle (including acquisition, development, and operations) and supply chain. In addition, past SEI research examined various types of risk, including software development risk [Dorofee 1996, Williams 1999, Alberts 2009], system acquisition risk [Gallagher 1999], operational risk [Gallagher 2005], mission risk [Alberts 2009] and information security risk [Alberts 2002], among others. A key result of our research into the practice of risk management was the development of the MRD, a mission-oriented approach for assessing risk in interactively complex, socio-technical systems.[1]

The overarching goal of the MRD is to determine the extent to which a system is in position to achieve its mission and objective(s) [Alberts 2012]. As shown in Figure 2, the MRD method can be applied in a variety of contexts, and to date we have piloted the MRD in the contexts of software acquisition and development, cybersecurity incident management, software security, software supply-chain, and business portfolio management, among others.

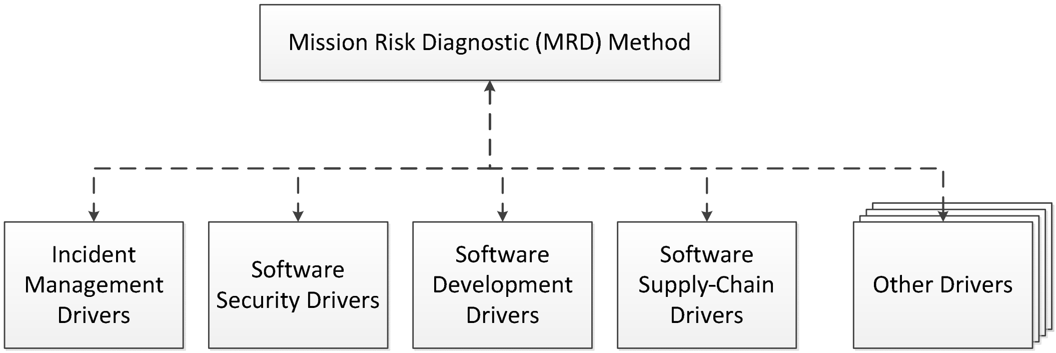

Mission Risk Diagnostic (MRD) Method
Incident Management Drivers
Software Security Drivers
Software Development Drivers
Software Supply-Chain Drivers
Other Drivers

Figure 1: Single Platform, Multiple Assessments

When we tailor the MRD method to a given context, we first develop and document a unique set of drivers (i.e., risk factors) for that context. We then integrate the drivers with the MRD method to produce a unique assessment. In this way, the MRD method provides a common platform for a family of related assessments. The MRD-IMC is one of the assessments in the MRD family.

1.2 Overview of the MRD-IMC

The MRD-IMC can be viewed as a first-pass screening (i.e., a "health check") or high-level diagnosis of conditions that enable and impede the successful completion of the IM function's mission. It provides a high-level assessment of an IM function, rather than a detailed, deep-dive

[1] A *socio-technical system* comprises interrelated technical and social elements (e.g., people who are organized in teams or departments, technologies on which people rely) that are engaged in goal-oriented behavior.

evaluation of IM processes and capabilities. The MRD-IMC comprises the following three core tasks:

1. **Identify the mission and objective(s)**—This task establishes the focus of the analysis and the specific aspects of the IM function that are important to decision makers. One or more objectives are identified during this activity.
2. **Identify drivers**—This task establishes a small set of critical factors (typically 10–25) that have a strong influence on whether or not the objective(s) will be achieved. These factors are called *drivers*.
3. **Analyze drivers**—The value of each driver is evaluated to determine how it is currently influencing performance. Next, the reasons underlying the evaluation of each driver (called the rationale) and any tangible evidence that supports the rationale are documented. Finally, a visual summary of the current values of all drivers relevant to the mission and objectives being assessed is documented.

Sections 2–4 of this report describe each of the core tasks in greater detail.

1.3 Purpose

The purpose of this document is to provide an overview of the MRD-IMC method. The content of this document supplements two previous method descriptions published by the SEI:

- *Incident Management Mission Diagnostic Method, Version 1.0* [Dorofee 2008]
- *Mission Risk Diagnostic (MRD) Method Description* [Alberts 2012]

This document updates the existing IMMD method description by providing a revised questionnaire for assessing an IM function. It also extends the MRD method description by providing a questionnaire that is tailored for cybersecurity incident management.[2] A more detailed MRD-IMC method description might be published at some point in the future. For now, this technical note provides enough information to supplement existing IMMD and MRD documentation and enables an experienced person or team to perform an MRD-IMC assessment.

1.4 Audience

The primary audience for this document is managers or senior staff members of IM functions who have a familiarity with risk management. People who have experience with or are interested in the following topics may also find this report useful:

- computer security incident management
- time- and resource-efficient methods for assessing and managing risk

It is assumed that readers will have an extensive familiarity with computer security incident management if they intend to use this method. Readers with an interest in risk management should also find the content of this report to be useful.

[2] The questionnaire featured in the MRD method description was developed for managing risk to a software-development project, not for managing risk to an IM function.

1.5 Structure of This Technical Note

This report comprises the following sections:

- *Section 2: Identify Mission and Objective(s)*—describes how to establish an IM function's mission and objective(s) and use them to set the scope of an MRD-IMC assessment
- *Section 3: Identify Drivers*—presents a set of risk factors, called drivers, which is derived from the IM function's mission and objective(s)
- *Section 4: Analyze Drivers*—describes how to analyze a set of drivers and present the results to stakeholders
- *Section 5: Applying the MRD-IMC*—discusses two approaches for applying the MRD-IMC: (1) an expert-led assessment and (2) a self-applied assessment
- *Section 6: Summary and Future Directions*—describes next steps in the development of the MRD-IMC
- *Appendix: MRD-IMC Workbook*—presents a workbook that can be used when conducting an MRD-IMC assessment

As discussed above, the MRD-IMC comprises the following three core tasks: (1) identify the mission and objective(s), (2) identify drivers, and (3) analyze drivers. The following sections of this report address each task in greater detail, beginning with the identification of the mission and objective(s) for the IM function that is being assessed.

2 Identify Mission and Objective(s)

The overarching goals when identifying the mission and objective(s) of an IM function are to (1) define the fundamental purpose, or mission, that will be assessed and (2) establish which specific aspects of that mission will be analyzed in detail. For the MRD-IMC, we defined the mission of an IM function as follows: *Continuous, enterprise-wide, and end-to-end management (detection, analysis, and response) of cyber events*[3] *and incidents*.[4] This mission is broad, requiring an IM function to complete the following range of activities:

- *Prepare*—Establish an effective, high-quality IM function.
- *Protect*—Take action to prevent attacks from happening and mitigate the impact of those that do occur.
- *Detect*—Collect and analyze information about current events, potential incidents, vulnerabilities, or other computer security or IM information. Detection is performed proactively and reactively.
- *Respond*—Take steps to analyze, resolve, or mitigate an event or incident.
- *Sustain*—Maintain and improve the IM function and the overall effectiveness of IM activities

After the mission has been established, the next step is to identify which specific aspects of the mission need to be analyzed in detail. An objective is defined as a tangible outcome or result that must be achieved when pursuing a mission. Each mission typically comprises multiple objectives. When assessing an IM function, analysts must select which specific objective(s) will be evaluated during the assessment. Selecting objectives refines the scope of the assessment to address the specific aspects of the mission that are important to decision makers.

We decided to focus our initial work on Detect and Respond (which also includes analysis of events and incidents). For the initial version of the MRD-IMC, we focused on the following objective that addresses Detect and Respond: *Each event or incident is managed effectively and in a timely manner*.

- *Delays in managing an event or incident are minimized.*
- *Damage to systems and networks is contained.*
- *Impact to operations and data is minimized.*

Once the mission and objective(s) are established, the next step is to identify a small set of critical factors that have a strong influence on whether or not the objective(s) will be achieved.

[3] An *event* is defined as an occurrence in a system or network that is relevant to security. An event is considered to be any type of suspicious system or network activity.

[4] An *incident* is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

3 Identify Drivers

The main goal of driver identification is to establish a set of systemic factors, called drivers, that can be used to measure performance in relation to an IM function's mission and objective(s). Once the set of drivers is established, analysts can then evaluate each driver in the set to gain insight into the likelihood of achieving the mission and objective(s). To measure performance effectively, analysts must ensure that the set of drivers conveys sufficient information about the mission and objective(s) being assessed.

A driver is a systemic factor that has a strong influence on the eventual outcome or result (i.e., whether or not objectives will be achieved). Deriving a unique set of drivers based on the mission and objective(s) requires gathering information from people with experience and expertise relevant to the specified mission and objectives. For example, identifying a set of drivers for software development objectives requires input from acquisition program managers and software-reliant systems developers. Similarly, analysts seeking to identify a set of drivers for IM would consult with people with IM expertise.

The experts from whom information is elicited should be familiar with the objective(s) that have been defined. Analysts can use the objectives to focus interviews or discussions with experts. During interviews or discussions, IM experts answer the following questions:

- What circumstances, conditions, and activities prevent an IM function from achieving each objective?
- What circumstances, conditions, and activities enable an IM function to achieve each objective?

The experts should consider a broad range of factors that can drive an IM function toward or away from its objective(s), including people, processes, work environment, and technology. After obtaining information from the experts, analysts organize the information into approximately 10–25 groups that share the driver as the central idea or theme of each group. The SEI has employed this approach for identifying drivers in a variety of areas, including software acquisition and development programs, cybersecurity processes, and business portfolio management.

When developing the set of drivers for the IM objective, we gathered data from several IM experts to produce the set of IM drivers shown in Table 1. Note that the drivers are phased as yes/no questions from the success perspective; an answer of yes indicates the driver is in its success state (i.e., driving the IM function toward its objectives) and an answer of no indicates it is in its failure state (i.e., driving the IM function away from its objectives).

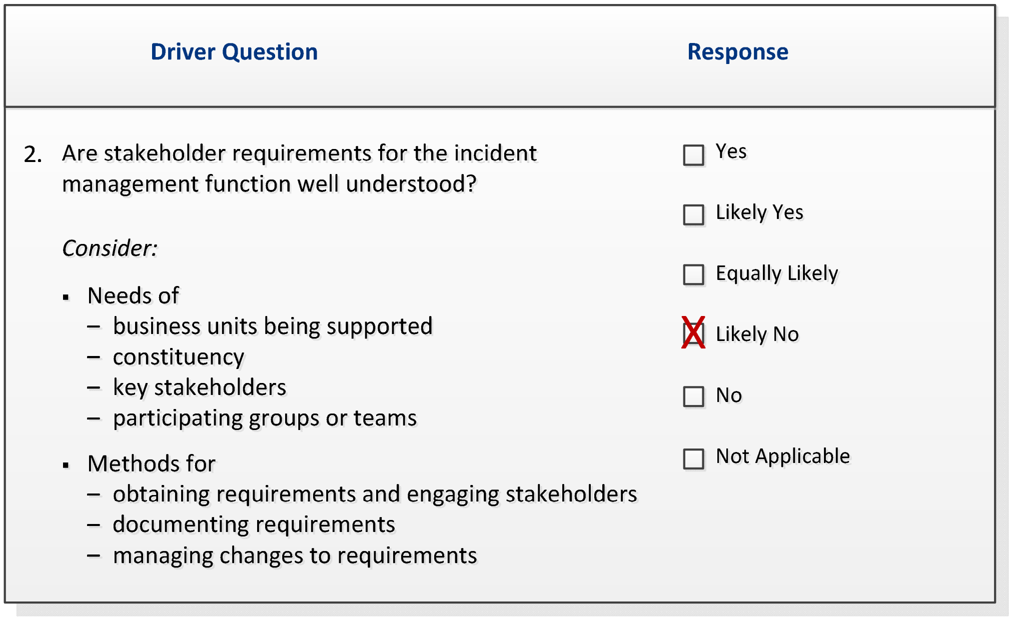
Table 1: MRD-IMC Driver Questions

Driver Name	Driver Question
1. Incident Management Objectives	Are the incident management function's objectives realistic and achievable?
2. Stakeholder Requirements	Are stakeholder requirements for the incident management function well understood?
3. Incident Management Plan	Does the incident management plan enable achievement of objectives?
4. Organizational Environment	Do organizational and political conditions facilitate the management of events and incidents?
5. People	Do people have sufficient knowledge, skills, and abilities to do their jobs?
6. Roles and Responsibilities	Do people understand their roles and responsibilities?
7. Information Management	Do people get the information they need when they need it?
8. Tools and Technologies	Do people have the tools and technologies they need to manage events and incidents effectively?
9. Facilities	Are facilities sufficient to support incident management activities?
10. Information Collection	Does the incident management function collect the information it needs to detect events and incidents?
11. Detection	Does the incident management function detect events and incidents in a timely manner?
12. Analysis	Does the incident management function analyze events and incidents sufficiently to enable an appropriate course of action for response?
13. Response	Does the incident management function respond to events and incidents sufficiently to minimize the impact to the business mission?
14. Information Dissemination	Does the incident management function disseminate relevant, timely, and accurate information to stakeholders?
15. Coordination	Does the incident management function coordinate management of events and incidents appropriately?
16. Resilience	Is the incident management function resilient to potential events and changing circumstances?

The next section of this document examines how to use the set of drivers to assess an IM function.

4 Analyze Drivers

The goal of driver analysis is to determine how each driver is influencing the objectives. More specifically, the analysis must establish the probability of a driver being in its success state or failure state. Each driver question in Table 1 is expressed as a yes/no question that is phrased from the success perspective. Figure 2 depicts a driver question for *Stakeholder Requirements*, the second question from Table 1.



Driver Question	Response
2. Are stakeholder requirements for the incident management function well understood? *Consider:* ▪ Needs of – business units being supported – constituency – key stakeholders – participating groups or teams ▪ Methods for – obtaining requirements and engaging stakeholders – documenting requirements – managing changes to requirements	☐ Yes ☐ Likely Yes ☐ Equally Likely ☒ Likely No ☐ No ☐ Not Applicable

Figure 2: Driver Question, Considerations, and Range of Responses

Because the question in Figure 2 is phrased from the success perspective, an answer of *yes* indicates the driver is in its success state and an answer of *no* indicates it is in its failure state. A range of answers is used to determine probabilities (likely yes, equally likely yes or no, likely no) when the answer is not a definitive yes or no. In addition, key items to consider when answering each question, called considerations, are provided for each driver question.

Figure 2 shows an example of an analyzed driver. The answer to the driver question is likely no, which means that the driver is most likely in its failure state. As a result, the needs of key stakeholders are not well understood, and as a result the IM objective will likely not be achieved.[5]

The rationale for the response to each driver question must also be documented because it captures the reasons why analysts selected the response. Any evidence supporting the rationale must also be cited as well. Examples of evidence include

- data from interviews of IM stakeholders
- IM documentation

[5] It is important to note that, by definition, a driver is a factor that is *critical* to achieving an objective. As a result, the driver has a direct influence on the achievement of the objective. If a driver is most likely in its failure state, then the objective will likely not be achieved.

- IM reports
- observations of people performing IM tasks
- measurement data

Recording the rationale and evidence is important for validating the data and associated information products, for historical purposes, and for developing lessons learned.

A *driver profile* provides a visual summary of the current values of all drivers relevant to the mission and objectives being assessed. A driver profile can be viewed as a dashboard that provides decision makers with a graphical summary of current conditions and expected performance in relation to the mission and objectives being pursued by the IM function. It depicts the probability that each driver is in its success state. Figure 3 provides an example of a driver profile for an IM function.

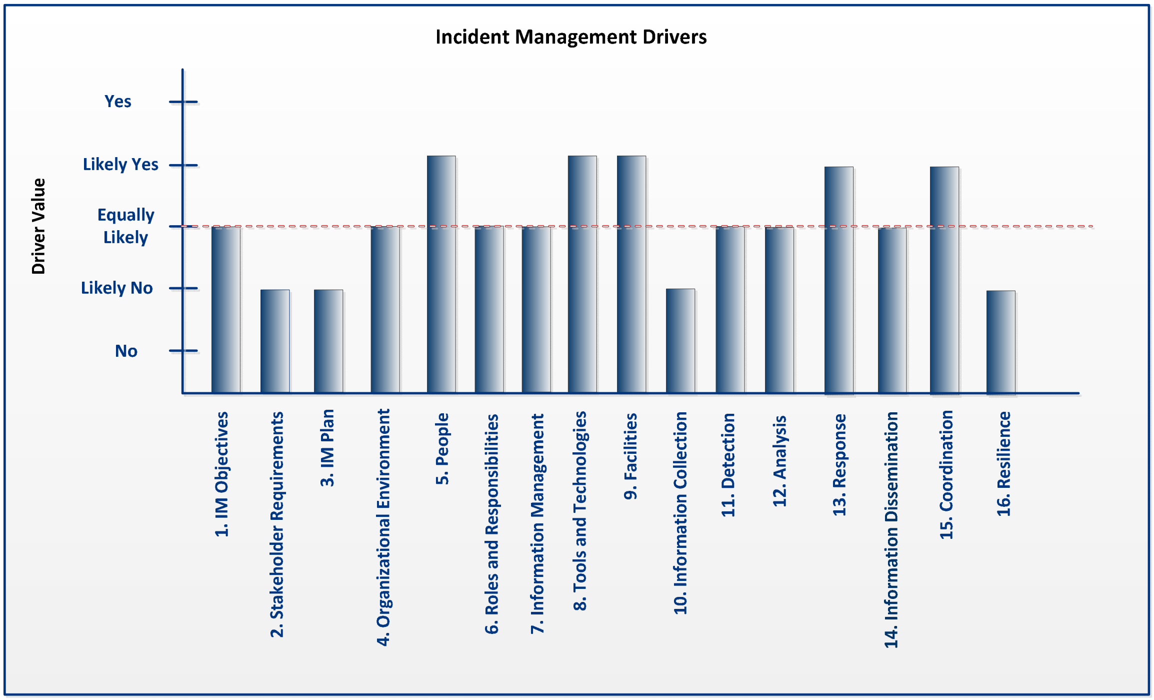


Figure 3: Driver Profile

Figure 3 uses a bar graph to show the 16 IM drivers. The profile in Figure 3 indicates that the following four drivers have a high probability of being in their failure states: Stakeholder Requirements, Incident Management Plan, Information Collection, and Resilience. The states of these four drivers should concern the program’s decision makers.

5 Applying the MRD-IMC

An MRD-IMC assessment can be expert-led or self-applied. Expert-led assessments are facilitated by a small team, called the assessment team, which is responsible for conducting the assessment and reporting its findings to stakeholders. The assessment team generally comprises three to five people who have a collective understanding of the technical and management aspects of IM as well as the ability to conduct an MRD-IMC assessment. During an expert-led assessment, the assessment team completes the following basic tasks:

- The team identifies groups of organizational peers (called participants) and assigns them to interview sessions. As a whole, participants must have knowledge of the IM function, its responsibilities, and its mission.
- The assessment team facilitates an interview session with each group. Participants in each session answer the driver questions individually (usually by completing a survey). The assessment team then facilitates a discussion of participants' answers. The assessment team documents the rationale for each answer as well as any supporting evidence that is cited by the participants.
- After all interview sessions are complete, the assessment team reviews the responses from each interview group. The team then answers each driver question based on its review of the individual responses. Team members discuss the answer to each driver question among themselves. This discussion can take time. Once consensus is reached, the team documents its answer, rationale, and supporting evidence for the driver question.
- The assessment team documents the results of the assessment, develops a driver profile, and communicates the results to the assessment's stakeholders.

Applying the MRD-IMC as a self-assessment is generally much simpler than conducting an expert-led assessment. Self-applied assessments tend to be much less formal then their expert-led counterparts. An individual or small team of people with knowledge of the IM function, its responsibilities, and its mission conducts the self-assessment. The individual or team

- answers each driver question and documents the rationale and supporting evidence for each answer
- documents a driver profile
- communicates the results to key stakeholders

A completed MRD-IMC assessment, whether expert-led or self-applied, provides stakeholders a high-level diagnosis (i.e., a "health check") of conditions that enable and impede the successful completion of the IM function's mission. IM stakeholders can then take action to improve current conditions when warranted and can conduct follow-on, deep-dive assessments to gather additional information when needed.

6 Summary and Future Directions

The MRD defines a time-efficient, mission-oriented approach for assessing risk in interactively complex, socio-technical systems. The overarching goal of an MRD assessment is to determine the extent to which a system is in position to achieve its mission and objectives. Over the past several years, we have tailored the MRD to a variety of contexts, including software acquisition and development, software security, software supply-chain, and business portfolio management, among others. In this technical note, we presented a version of the MRD that was developed for cybersecurity incident management. The result assessment, called the MRD-IMC, provides a high-level diagnosis of conditions that enable and impede the successful completion of an IM function's mission and objectives. As part of this development effort, we defined a set of risk factors, or drivers, to assess an IM function's ability to detect and respond to cyber events and incidents.

When we began the MRD-IMC project we wanted to achieve two key outcomes. First, we wanted to provide an update to the existing IMMD method, which was originally developed in 2008. Second, we were hoping to extend the MRD family of assessments by providing a version of the MRD method tailored for cybersecurity incident management. With the publication of this technical note, we have achieved both outcomes.

At the same time, we view this publication as an initial step in the development of the MRD-IMC rather than the culmination of our work in this area. We have identified a range of potential future development and transition tasks related to the MRD-IMC, including the following:

- Pilot the current version of the MRD-IMC with organizations throughout the IM community.
- Refine the current version of the MRD-IMC method based on pilot results.
- Develop additional sets of drivers for the Prepare, Protect, and Sustain activities performed by IM functions.
- Develop and document detailed guidance for applying the MRD-IMC (for expert-led assessments and self-assessments).
- Develop training for the MRD-IMC (for expert-led assessments and self-assessments).
- Extend and align the MRD-IMC to be consistent with new or updated community standards, practices, methods, frameworks, and tools for managing cybersecurity events and incidents.

Future development and transition activities will ultimately be determined by the feedback that we receive from people throughout the IM community. No matter which path is followed, we believe that the body of work presented in this technical note is an important step forward in helping organizations to build an IM function and sustain it over time.

Appendix: MRD-IMC Workbook

This appendix provides a workbook for conducting the Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC). The workbook incorporates the standard set of drivers for detecting, analyzing, and responding to cyber events and incidents. The MRD-IMC workbook is divided into two parts:

- Part 1 provides worksheets for analyzing the current state of each driver.
- Part 2 provides a worksheet for summarizing the results of Part 1 in a graphical driver profile format.

Part 1: Analyzing Driver State

Directions:

1. Review the following three items for Part 1: (1) the mission and objective for detecting and responding to incidents, (2) the driver value criteria, and (3) the driver-question worksheets.

   Refer to the *Part 1 Example* to see what the results for Part 1 look like.

2. Select a driver to analyze. Review the corresponding driver question and considerations. Select the most appropriate response to the driver question (keeping in mind the mission and objective for incident management). Refer to the driver value criteria for a definition of each response, if needed.
3. Document the rationale for your response to the driver question.
4. Complete steps 2 and 3 for all drivers.

Incident Management Mission

Continuous, enterprise-wide, and end-to-end management (detection, analysis, and response) of cyber events and incidents

Incident Management Objective

Each event or incident is managed effectively and in a timely manner.

- Delays in managing an event or incident are minimized.
- Damage to systems and networks is contained.
- Impact to operations and data is minimized.

Driver Value Criteria

Response	Definition
Yes	The answer is almost certainly “yes.” Almost no uncertainty exists. There is little or no probability that the answer could be “no.”
Likely Yes	The answer is most likely “yes.” There is some chance that the answer could be “no.”
Equally Likely	The answer is just as likely to be “yes” or “no.”
Likely No	The answer is most likely “no.” There is some chance that the answer could be “yes.”
No	The answer is almost certainly “no.” Almost no uncertainty exists. There is little or no probability that the answer could be “yes.”
Not Applicable	The driver question is not relevant at this point in time. It was not evaluated.

Part 1 Example

1. Incident Management Objectives

Driver Question	Response	Rationale
Are the incident management function’s objectives realistic and achievable? Consider: ▪ Success criteria and measures for incident management ▪ Requirements of key stakeholders ▪ Incident management services offered ▪ Organizational constraints – Resources (e.g., people, technologies) available – Funding ▪ External constraints (e.g., regulatory, legal) ▪ Incident management policy, plan, processes, and procedures	□ Yes □ Likely Yes ☒ Equally Likely □ Likely No □ No □ Not Applicable	+ The CSIRT has a good sense of its requirements and responsibilities. + Technical objectives sufficiently consider constituency needs. - The current set of objectives for the standard services to be provided to constituents is not documented or well communicated to the two contractors. - Plans for improving the CSIRT’s services are documented to some extent, but the schedule is out of date.

Driver-Question Worksheets

1. Incident Management Objectives

Driver Question	Response	Rationale
Are the incident management function’s objectives realistic and achievable? Consider: ▪ Success criteria and measures for incident management ▪ Requirements of key stakeholders ▪ Incident management services offered ▪ Organizational constraints – Resources (e.g., people, technologies) available – Funding ▪ External constraints (e.g., regulatory, legal) ▪ Incident management policy, plan, processes, and procedures	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

2. Stakeholder Requirements

Driver Question	Response	Rationale
Are stakeholder requirements for the incident management function well understood? Consider: ▪ Needs of – business units being supported – constituency – key stakeholders – participating groups or teams ▪ Methods for – obtaining requirements and engaging stakeholders – documenting requirements – managing changes to requirements	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

3. Incident Management Plan

Driver Question	Response	Rationale
Does the incident management plan enable achievement of objectives? Consider: ▪ Business priorities of the organization ▪ Incident management services provided ▪ Roles, responsibilities, and reporting structure ▪ Plans for communication, data management, and training ▪ Guidelines/processes for – coordinating incidents – managing incidents throughout their lifecycles – involving other groups (e.g., legal, public relations) – postmortem analysis ▪ Resources, budget, and projected costs ▪ Common incident scenarios and mitigation approaches documented in the plan ▪ Institutionalization of the incident management plan *Note*: Some organizations use the term *incident response plan* instead of *incident management plan*.	❑ Yes ❑ Likely Yes ❑ Equally Likely ❑ Likely No ❑ No ❑ Not Applicable	

4. Organizational Environment

Driver Question	Response	Rationale
Do organizational and political conditions facilitate the management of events and incidents? Consider: ▪ Relationship between incident management function and the business units ▪ Stakeholder sponsorship of incident management ▪ Designated authority of the incident management function ▪ Actions of organizational managers ▪ Organizational or interorganizational culture and politics ▪ Effect of organizational or interorganizational bureaucracy ▪ Effect of laws, regulations, and policies ▪ Effect of contracts and agreements (e.g., service level agreements, nondisclosure agreements)	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

5. People

Driver Question	Response	Rationale
Do people have sufficient knowledge, skills, and abilities to do their jobs? Consider: ▪ Extent to which knowledge, skills, and abilities (i.e., competencies) for job assignments are established and documented ▪ People’s readiness to perform their job assignments (includes proper background, training, and experience) ▪ Effectiveness of training provided ▪ People’s knowledge of the business and incident management missions ▪ Ability to use tools and technologies ▪ Ability to access subject matter experts when appropriate ▪ Flexibility and resourcefulness of workforce	❑ Yes ❑ Likely Yes ❑ Equally Likely ❑ Likely No ❑ No ❑ Not Applicable	

6. Roles and Responsibilities

Driver Question	Response	Rationale
Do people understand their roles and responsibilities? Consider: ▪ Extent to which roles and responsibilities are established and documented ▪ Appropriateness of people's background and experience to their assigned roles and responsibilities ▪ Extent to which organizational culture and procedures facilitate execution of roles and responsibilities ▪ Timeliness and effectiveness of training for roles and responsibilities ▪ Frequency of refresher training for roles and responsibilities ▪ Ability to coordinate work tasks across roles as appropriate ▪ Measures for ensuring that roles and responsibilities do not conflict (i.e., deconfliction of roles and responsibilities) ▪ Institutionalization of roles and responsibilities across the enterprise ▪ Extent to which people have authority to complete their job assignments	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

7. Information Management

Driver Question	Response	Rationale
Do people get the information they need when they need it? Consider: ▪ Availability, timeliness, and usability requirements for information ▪ Strategy for disseminating information to people (as documented in the incident management plan) ▪ Workflows for information collection and analysis (as defined in the incident management plan and processes) ▪ Coordination of incident management activities among participating groups or teams ▪ Extent to which information systems and technologies provide people with the information they need when they need it ▪ Effect of mechanisms for protecting information during processing, storage, and transmission ▪ Effect of information management classification schema on information handling	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

8. Tools and Technologies

Driver Question	Response	Rationale
Do people have the tools and technologies they need to manage events and effectively? Consider: ▪ Extent to which tools and technologies support and automate incident management activities (e.g., ticketing system, central repository, operations log) ▪ Ability to set up, use, and tailor tools and technologies ▪ Effectiveness of training for tools and technologies ▪ Timeliness of training for tools and technologies ▪ Frequency of refresher training for tools and technologies ▪ Extent to which incident management tools and technologies are securely configured ▪ Protection of information during processing, storage, and transmission ▪ Effect of security mechanisms on the performance of tools and technologies	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

9. Facilities

Driver Question	Response	Rationale
Are facilities sufficient to support incident management activities? Consider: ▪ Physical and personnel security requirements needed to support incident management ▪ Protective measures that are in place (including physical access controls) ▪ Physical work spaces used for incident management ▪ Individual work spaces used for incident management ▪ Physical space (with controlled access) for storage of sensitive or confidential data ▪ Access to equipment and facility for secure communications (such as a SCIF, if needed)	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

10. Information Collection

Driver Question	Response	Rationale
Does the incident management function collect the information it needs to detect events and incidents? Consider: ▪ Ability to monitor systems and networks ▪ Ability to keep up with public sources of information (e.g., external websites, trusted sources of information) ▪ Ability to coordinate information collection activities ▪ Ability to collect, preserve, document, and analyze evidence from a compromised computer system or component ▪ Ability to analyze and correlate logs ▪ Situational awareness capabilities ▪ Reporting mechanisms for events and incidents (e.g., guidelines for reporting events and incidents, reporting forms) ▪ Methods and techniques for collecting information ▪ Training for information collection ▪ Tools and technologies that support and automate information collection activities ▪ Resources allocated to information collection	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

11. Detection

Driver Question	Response	Rationale
Does the incident management function detect events and incidents in a timely manner? Consider: ▪ Criteria and/or thresholds for incident declaration ▪ Existence of categories and priority ranking of events and incidents ▪ Ability to detect abnormal conditions and events ▪ Ability to detect potential incidents ▪ Ability to detect multiple, simultaneous events or incidents ▪ Ability to recognize false positives ▪ Ability for constituents to report suspicious events ▪ Training for detection activities ▪ Tools and technologies that support and automate detection activities ▪ Resources allocated to detection	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

12. Analysis

Driver Question	Response	Rationale
Does the incident management function analyze events and incidents sufficiently to enable an appropriate course of action for response? Consider: ▪ Ability to initiate appropriate response activities ▪ Ability to prevent future occurrences of similar events and incidents ▪ Ability to collect, preserve, document, and analyze evidence from a compromised computer system, network, or component ▪ Ability to analyze an event or incident (e.g., what occurred, extent of damage, which computers are involved, cause of event or incident, timing of the event) ▪ Ability to correlate data ▪ Ability to perform or have access to subject matter experts (SMEs) who can perform the following: – Digital media analysis – Vulnerability analysis – Forensic evidence collection – Malware analysis ▪ Ability to determine the root cause of an event or incident ▪ Ability to analyze trends and perform predictive analysis ▪ Ability to coordinate analysis activities ▪ Training for analysis activities ▪ Tools and technologies that support and automate analysis activities ▪ Resources allocated to analysis	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

13. Response

Driver Question	Response	Rationale
Does the incident management function respond to events and incidents sufficiently to minimize the impact to the business mission? Consider: ▪ Ability to provide direct, on-site assistance to constituents ▪ Ability to respond to events and incidents on remote systems ▪ Ability to coordinate response activities ▪ Ability to mitigate or repair vulnerabilities ▪ Ability to contain the spread of malicious activity ▪ Ability to eliminate the root cause of an event or incident when appropriate ▪ Ability to locate and remove compromised artifacts from a system ▪ Ability to restore systems to a known, trusted state and recover information as appropriate ▪ Training for response activities ▪ Tools and technologies that support and automate response activities ▪ Resources allocated to response	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

14. Information Dissemination

Driver Question	Response	Rationale
Does the incident management function disseminate relevant, timely, and accurate information to stakeholders? Consider: ▪ Bulletins, warnings, and alerts provided to stakeholders ▪ Information sharing with partners and collaborators ▪ Content of briefings to management ▪ Notification services ▪ Guidance for utilizing information ▪ Training for information dissemination activities ▪ Tools and technologies that support and automate information dissemination ▪ Resources allocated to information dissemination	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

15. Coordination

Driver Question	Response	Rationale
Does the incident management function coordinate management of events and incidents appropriately? Consider: ▪ Communication plan ▪ Contracts and agreements with participating groups or teams (e.g., service level agreements, memorandums of understanding, nondisclosure agreements) ▪ Ability to coordinate detection, analysis, and response activities ▪ Working relationships with participating groups or teams, including – victim(s) of the attack, including affected sites and organizations – system and network administrators – data owners – service providers and vendors – security groups (cyber and physical) – subject matter experts (SMEs) – trusted groups (e.g., US-CERT, GFIRST, Information Sharing and Analysis Centers) – law enforcement – public relations, human resources, business units, and other parts of the organization as needed ▪ Information-sharing practices with participating groups or teams ▪ Tools and technologies that support and automate coordination ▪ Resources allocated to coordination	□ Yes □ Likely Yes □ Equally Likely □ Likely No □ No □ Not Applicable	

16. Resilience

Driver Question	Response	Rationale
Is the incident management function resilient to potential events and changing circumstances? Consider: ▪ Continuity and contingency plans for incident management function ▪ Disaster recovery plans for incident management function ▪ Risks to the success of the incident management mission ▪ Risk mitigation plans ▪ Process resilience ▪ Staff resilience ▪ Ability of staff to adapt to novel situations ▪ Cross training of staff ▪ Ability to access subject matter experts (SMEs) as needed ▪ Ability to manage surges in workload ▪ Reliability and resilience of tools and technologies (e.g., alternative communication systems, mirrored sites) ▪ Track record of improving the incident management function based on lessons learned	❑ Yes ❑ Likely Yes ❑ Equally Likely ❑ Likely No ❑ No ❑ Not Applicable	

Part 2: Documenting the Driver Profile

Directions:

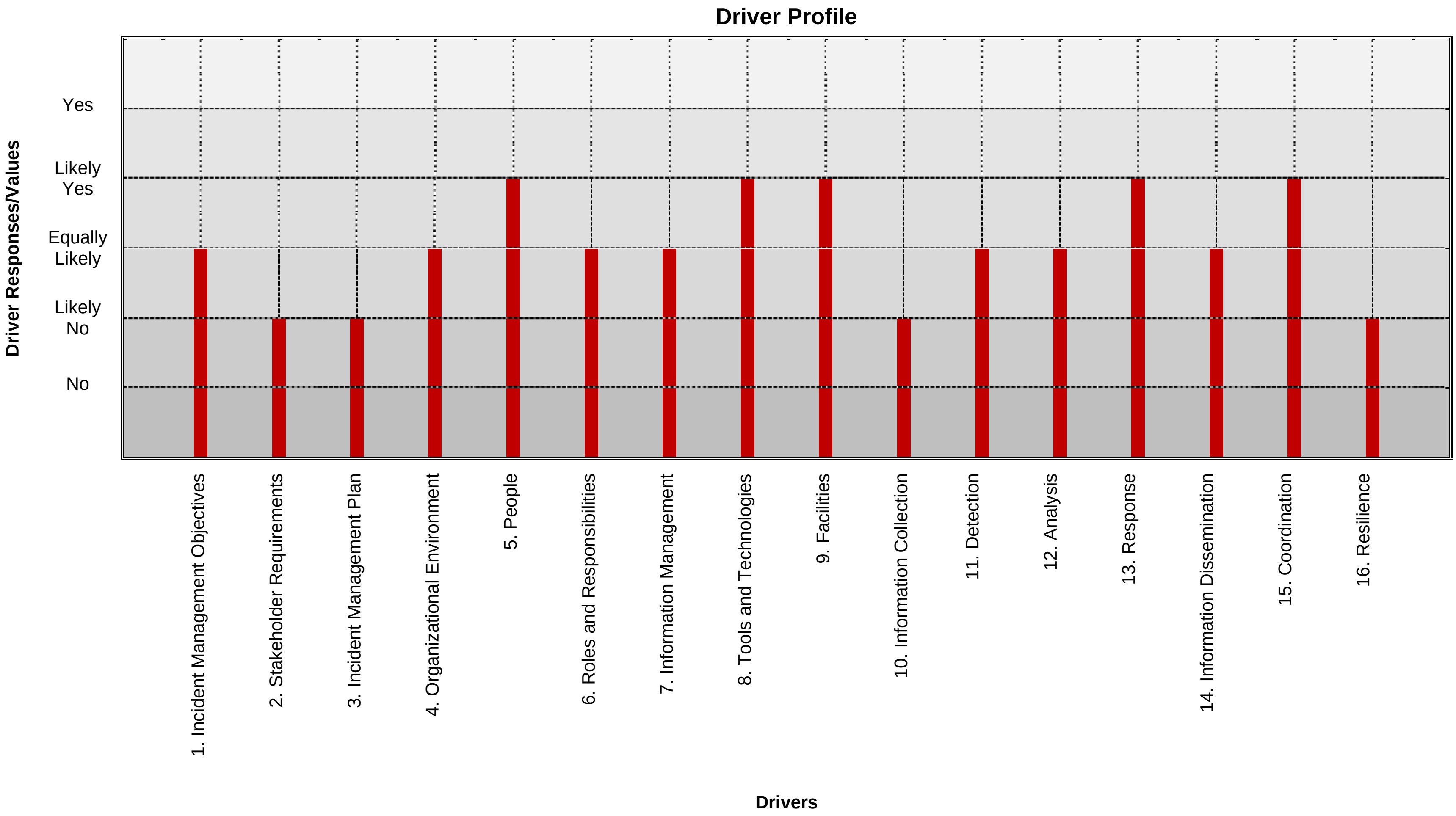
1. The driver profile featured in Part 2 provides a graphical snapshot of an incident management function's current state, where the value of each driver is plotted on a bar chart.

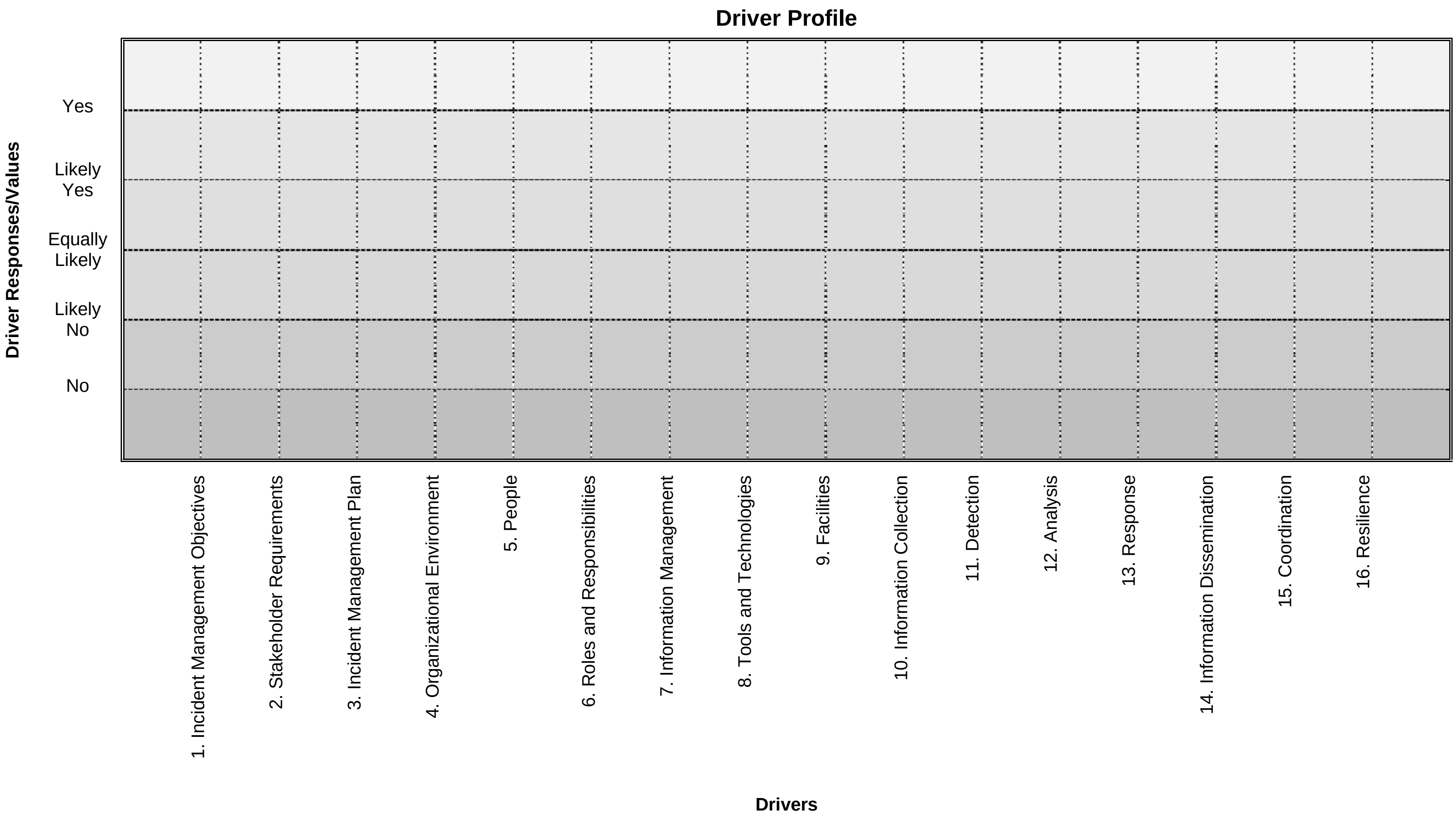
   Refer to *Part 2 Example* to see what the results for Part 2 look like.

2. Complete the driver profile using results from Part 1 of this workbook.

   If your response to any driver question in Part 1 was *Not Applicable*, you should leave the bar for that driver blank.

Part 2 Example




Driver Profile
Driver Responses/Values
Yes
Likely Yes
Equally Likely
Likely No
No
1. Incident Management Objectives
2. Stakeholder Requirements
3. Incident Management Plan
4. Organizational Environment
5. People
6. Roles and Responsibilities
7. Information Management
8. Tools and Technologies
9. Facilities
10. Information Collection
11. Detection
12. Analysis
13. Response
14. Information Dissemination
15. Coordination
16. Resilience
Drivers

Glossary

assessment team
a small team of people responsible for conducting the assessment and reporting its findings to stakeholders

constituency
a defined group supported by an incident management function. A constituency can be multiple commercial organizations, one parent organization, or organizations within a particular geographic region, etc.

driver
a systemic factor that has a strong influence on the eventual outcome or result (i.e., whether or not objectives will be achieved)

driver analysis
an approach for determining how each driver is influencing the objectives

driver identification
an approach for establishing a set of systemic factors, called drivers, that can be used to measure performance in relation to a system's mission and objectives

driver profile
a visual summary of the current values of all drivers relevant to the mission and objectives being assessed

event
an occurrence in a system or network that is relevant to security. An event is considered to be any type of suspicious system or network activity.

failure state
the condition of a driver when it exerts a negative influence on the outcome; one of two possible states a driver can assume

incident
a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

incident management (IM) function
the broad spectrum of everything associated with providing incident management services. An incident management function is instantiated in a set of capabilities (or practices) considered essential to protecting, detecting, and responding to incidents, as well as sustaining the IM function. These capabilities can be provided internally by security or network operators, be outsourced, or be provided and managed by a computer security incident response team (CSIRT).

interactive complexity
the presence of unplanned and unexpected sequences of occurrences in a system that are either not visible or not immediately understood

interactively complex system
a system whose components interact in relatively unconstrained ways

mission
the fundamental purpose of the system that is being examined

mission risk
the probability of mission failure (i.e., not achieving key objectives); the probability that a driver is in its failure state

mission risk analysis
a risk analysis that examines the aggregate effects of multiple conditions and events on a system's ability to achieve its mission

Mission Risk Diagnostic (MRD)
an approach for assessing mission risk in interactively complex, socio-technical systems, such as projects, programs, and processes

mitigation
any action taken to address a risk

objective
a tangible outcome or result that must be achieved when pursuing a mission; defines specific aspects of the mission that are important to decision makers

process
a collection of interrelated work tasks that achieves a specific result

program
a group of related projects managed in a coordinated way to obtain benefits and control not available from managing them individually; programs usually include an element of ongoing activity

project
a planned set of interrelated tasks to be executed over a fixed period of time and within certain cost and other limitations

risk
the probability of suffering harm or loss

risk management
a systematic approach for minimizing exposure to potential losses

socio-technical system

interrelated technical and social elements (e.g., people who are organized in teams or departments, technologies on which people rely) that are engaged in goal-oriented behavior

software-reliant system

a socio-technical system whose behavior (e.g., functionality, performance, safety, security, interoperability, and so forth) depends on software in some significant way

success state

the condition of a driver when it exerts a positive influence on the outcome; one of two possible states a driver can assume

task

a piece of work that must be completed when performing an assessment activity

References

URLs are valid as of the publication date of this document.

[Alberts 2002]
Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE^{SM} Approach*. Addison-Wesley, 2002.
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=30678

[Alberts 2009]
Alberts, Christopher & Dorofee, Audrey. *A Framework for Categorizing Key Drivers of Risk* (CMU/SEI-2009-TR-007). Software Engineering Institute, Carnegie Mellon University, 2009.
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9093

[Alberts 2012]
Alberts, Christopher & Dorofee, Audrey. *Mission Risk Diagnostic (MRD) Method Description* (CMU/SEI-2012-TN-005). Software Engineering Institute, Carnegie Mellon University, 2012.
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=10075

[Dorofee 1996]
Dorofee, A.; Walker, J.; Alberts, C.; Higuera, R.; Murphy, R.; & Williams, R. *Continuous Risk Management Guidebook*. Software Engineering Institute, Carnegie Mellon University, 1996.
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=30856

[Dorofee 2008]
Dorofee, A.; Killcrece, G.; Ruefle, R.; & Zajicek, M. *Incident Management Mission Diagnostic Method, Version 1.0* (CMU/SEI-2008-TR-007). Software Engineering Institute, Carnegie Mellon University, 2008. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8683

[Gallagher 1999]
Gallagher, Brian. *Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook Version 1.02* (CMU/SEI-99-HB-001). Software Engineering Institute, Carnegie Mellon University, 1999. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=13165

[Gallagher 2005]
Gallagher, B.; Case, P.; Creel, R.; Kushner, S.; & Williams, R. *A Taxonomy of Operational Risks* (CMU/SEI-2005-TN-036). Software Engineering Institute, Carnegie Mellon University, 2005.
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=7525

[Williams 1999]
Williams, R.; Pandelios, G.; & Behrens, S. *Software Risk Evaluation (SRE) Method Description (Version 2.0)* (CMU/SEI-99-TR-029). Software Engineering Institute, Carnegie Mellon University, 1999. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=13557

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY
(Leave Blank)

2. REPORT DATE
May 2014

3. REPORT TYPE AND DATES COVERED
Final

4. TITLE AND SUBTITLE
An Introduction to the Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC)

5. FUNDING NUMBERS
FA8721-05-C-0003

6. AUTHOR(S)
Christopher Alberts, Audrey Dorofee, Robin Ruefle, Mark Zajicek

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2014-TN-005

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFLCMC/PZE/Hanscom
Enterprise Acquisition Division
20 Schilling Circle
Building 1305
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

An incident management (IM) function is responsible for performing the broad range of activities associated with managing computer security events and incidents. For many years, the Software Engineering Institute's (SEI) CERT® Division has developed practices for building and sustaining IM functions in government and industry organizations worldwide. Based on their field experiences over the years, CERT researchers identified a community need for a time-efficient means of assessing an IM function. The Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC) is designed to address this need. The MRD-IMC is a risk-based approach for assessing the extent to which an IM function is in position to achieve its mission and objectives. Analysts applying the MRD-IMC evaluate a set of systemic risk factors (called drivers) to aggregate decision-making data and provide decision makers with a benchmark of an IM function's current state. The resulting gap between the current and desired states points to specific areas where additional investment is warranted. The MRD-IMC can be viewed as a first-pass screening (i.e., a "health check") or high-level diagnosis of conditions that enable and impede the successful completion of the IM function's mission and objectives. This technical note provides an overview of the MRD-IMC method.

14. SUBJECT TERMS
Mission Risk Diagnostic, MRD, incident management, incident management function, incident management capabilities, incident handling, incident response, computer security, CSIRT, risk, risk analysis

15. NUMBER OF PAGES
52

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UL